REMARKS / ARGUMENTS

The present application includes pending claims 1-7, 9-24, and 26-43. Claims 1-7, 9-24, and 26-28 have been rejected. By this Amendment, claims 8 and 25 have been cancelled, and claims 1, 10, 18, 20-24, and 26-28 have been amended to further clarify the language. New claims 29-43 have been added. The Applicant respectfully submits that the claims define patentable subject matter.

Claims 8 and 25 have been objected to. Claims 11-17 are rejected under 35 U.S.C. § 102(e) as anticipated by or, in the alternative, under 35 U.S.C. § 103(a) as obvious over Paila (USPN 2004/0072557).

Claims 1-3, 6, 10-13, 18-20, 23, and 27-28 are rejected under 35 U.S.C. § 102(e) as anticipated by Birell (USPN 5805803).

Claims 1-4, 6-7, 10-13, 18-21, 23-24, and 27-28 are rejected under 35 U.S.C. § 103(a) as obvious over Birell (USPN 5805803).

Claims 1, 3, 6-7, 11-13, 18, 20, and 23-24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Handelman (USPUB 2004/0016002).

Claims 5 and 22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Handelman in view of Stallings (William Stallings, "Network Security Essentials: Applications and Standards", ISBN: 0130160938, 2000).

The Applicant respectfully traverses these rejections at least based on the following remarks.

REJECTION UNDER 35 U.S.C. § 102

I. Paila Does Not Anticipate Claims 11-17

The Applicant first turns to the rejection of claims 11-17 under 35 U.S.C. 102(e) as being anticipated by Paila. Without conceding that Paila qualifies as prior art under 35 U.S.C. 102(e), the Applicant respectfully traverses this rejection as follows.

With regard to the anticipation rejections under 102, MPEP 2131 states that "[a] claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See Manual of Patent Examining Procedure (MPEP) at 2131 (internal citation omitted). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." See id. (internal citation omitted).

A. Rejection of Independent Claim 11

With regard to the rejection of independent claim 11 under 35 U.S.C. § 102(e) (or, in the alternative, under 35 U.S.C. § 103(a)), the Applicant submits that Paila does not disclose or suggest at least the limitation of "detecting by the node when the media peripheral is communicatively coupled to the node," as recited by the Applicant in independent claim 11.

The Office Action states the following:

> In Fig. 3 (and associated text) Paila discloses facilitating secure communication between the media peripheral and the communication network (Paila, [0053-0055]) that includes detecting by the node when the media peripheral is communicatively coupled to the node (action A2 and

> associated text, for example), utilizing acquired by the node, upon said detection, security data associated with the media peripheral (M2 includes MN_NAI identifying MN, the home domain and authority AAAH, for example, Paila, [0037-0040]) and utilizing security data associated with the node (e.g. the AAAL must receive at least some identification of ATT; otherwise sending data back to ATT, as indicated by the disclosure of step A8 would not be possible).

See the Office Action at page 3. Referring to FIGS. 4-6 of Paila, the AAAL server (equated by the Examiner to Applicant's "node") communicates a service advertisement message M1 during action A1. *See* Paila at paragraphs 0022-0032. During action A2, the mobile node (equated by the Examiner to Applicant's "media peripheral") communicates back a service request message M2, thereby selecting one of the service offerings specified in the service advertisement message M1. *See id.* at paragraphs 0033-0041. In this regard, Paila does not disclose that the AAAL server performs any detection of the mobile node during either action A1 or A2. On the contrary, the mobile node detects the AAAL (and not vice versa) by virtue of the received service advertisement message M1 during action A1. Therefore, the Applicant maintains that Paila does not disclose or suggest at least the limitation of "detecting by the node when the media peripheral is communicatively coupled to the node," as recited by the Applicant in independent claim 11.

Furthermore with regard to the rejection of independent claim 11 under 35 U.S.C. § 102(e) (or, in the alternative, under 35 U.S.C. § 103(a)), the Applicant submits that Paila does not disclose or suggest at least the limitation of "acquiring by the node, upon said detection, security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 11.

The Office Action states the following:

> Paila does not explicitly disclose that the security data is associated with location of previous operation of the media peripheral. However, the main purpose of portable devices (such as media peripherals disclosed by Paila) is to operate within the home domain. Thus, operating the peripheral in peripheral's home domain preceding operating the peripheral in a foreign domain (equating the security data comprising MN_NAI value to "a location of the previous operation of the media peripheral"), if not inherent, would have been at least implicit.

See the Office Action at pages 3-4. The Examiner concedes that Paila does not explicitly disclose that the security data is associated with location of previous operation of the media peripheral, and alleges the missing limitation is inherent or implicit. The Applicant respectfully disagrees. Initially, the Applicant points out that **Paila only discloses a "mobile node" (MN) and does not even disclose a media peripheral**, as alleged by the Examiner.

Furthermore, the Examiner's statement that "the main purpose of portable devices (such as media peripherals disclosed by Paila) is to operate within the home domain" is **not** supported by Paila. On the contrary, Paila discloses a mobile node (such as a cell phone), which can operate not only in a home domain but in one or more foreign domains. *See* Paila at, e.g., paragraph 0007. **Even if we assume for the sake of argument that Paila's mobile node is a media peripheral with a "main purpose" to operate within the home domain, the Examiner's argument above is still deficient. More specifically, "operating the peripheral in peripheral's home domain preceding operating the peripheral in a foreign domain" would be neither inherent nor implicit. As stated in paragraph 0007 of Paila, the mobile node may**

operate in several foreign domains. Therefore, in an exemplary scenario, the mobile node may leave the home domain, operate in a first foreign domain, then operate in a second foreign domain, etc. In other words, "operating the peripheral in peripheral's home domain preceding operating the peripheral in a foreign domain" is neither inherent nor implicit since the mobile node may successively operate in many foreign domains.

Therefore, the Applicant maintains that Paila does not disclose or suggest at least the limitation of "acquiring by the node, upon said detection, security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 11.

Accordingly, independent claim 11 is not anticipated by (or unpatentable over) Paila and is allowable.

B. Rejection of Dependent Claims 12-17

Based on at least the foregoing, the Applicant believes the rejection of independent claim 11 under 35 U.S.C. § 102(e) as being anticipated by (or under 35 U.S.C. § 103(a) as being unpatentable over) Paila has been overcome and request that the rejection be withdrawn. Additionally, claims 12-17 depend from independent claim 11 and are, consequently, also respectfully submitted to be allowable.

Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 11-17.

II. Birrell Does Not Anticipate Claims 1-3, 6, 10-13, 18-20, 23, and 27-28

The Applicant now turns to the rejection of claims 1-3, 6, 10-13, 18-20, 23, and 27-28 under 35 U.S.C. 102(e) as being anticipated by Birrell. Without conceding that Birrell qualifies as prior art under 35 U.S.C. 102(e), the Applicant respectfully traverses this rejection as follows.

A. Rejection of Independent Claims 1, 11, and 18

With regard to the rejection of independent claim 1 under 35 U.S.C. § 102(e), the Applicant submits that Birrell does not disclose or suggest at least the limitation of "searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 1.

The Office Action states the following:

> In col. 4 lines 18-27 Birrell discloses:
>
> "(13) At this point, if the client 110 is already known to the proxy server, then proceed with message 209, i.e., request 370 below. Otherwise, in the case where the client is unknown, the redirected browser makes a secure request 330 in a message 203 to the proxy server 143 for the desired resource. In the case, where the client 110 is unknown, the proxy server 143 replies a message 204 to demand that the user makes an authentication request 205 using the checker 141, e.g., a redirect 340 to the checker 141."
>
> This reads on: "searching by the node, for a previously acquired security data" associated with a location of previous operation of the media peripheral.

See the Office Action at pages 5-6. In page 5 of the Office Action, the Examiner equates Applicant's "node" and "media peripheral" to Birrell's tunnel 140 and client 110.

In reference to the above Birrell citation used by the Examiner (col. 4, lines 18-27), the Applicant points out that the tunnel 140 (or any of its modules – checker 141, redirector 142, or proxy 143) does not perform any searching whatsoever. In addition, the only "security data" being exchanged between the client 110 and the tunnel 140 are secure tokens, which are being used for purposes of authenticating the connection. *See* Birrell at FIGS. 2-3. Birrell simply does not disclose that the tunnel 140 performs any searching for a previously acquired security data, which is associated with a location of previous operation of the client 110.

Therefore, Birrell does not disclose or suggest at least the limitation of "searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 1.

Furthermore with regard to the rejection of independent claim 1 under 35 U.S.C. § 102(e), the Applicant submits that Birrell does not disclose or suggest at least the limitation of "if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network," as recited by the Applicant in independent claim 1.

The Office Action states the following:

> Similarly, col. 4 lines 18-27 with
> "As a result of the interchanges with the checker 141, the client computer can be provided, in step 360, a validation token 299 in message 208. The

> token can be in the form of an X.500 certificate. Alternatively, the token 299 can be a short-term password to authenticate the user on the HTTPS connection. The short-term password might automatically get installed in the client 110 as a Web "cookie" as a side-effect of the interchange. The message 208 also redirects the browser 111 to further communicate with the proxy server 143.
>
> Therefore, in a next message 209, the client send the request for the resource plus the token 299 to the proxy server 143. When the proxy server 143 receives the message, it validates the token 299. If the token is valid, then the proxy server 143 behaves as a conventional proxy server.
>
> The proxy server 143 forwards the authenticated request 210 to the specified resource 160 inside the firewall 130 using the non-secure HTTP protocol. The resource 160 replies to the request with, for example private data, in message 211. The proxy server 143 then forwards the data, using secure HTTPS protocol, in a message 212 (step 380).
>
> Subsequent requests for private resources during the session can be handled as follows. The resource is specified in a public message 201 to the redirector 142. The redirector replies message 202. The client 110 now in possession of the token 299 replies message 208 (step 370) causing the further interchange of message 210-212 between the proxy and the server controlling the private resource 160. "
>
> as taught in col. 4 lines 37-64, reads on: "if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network".

See the Office Action at pages 6-7. As already explained above in reference to Birrell's FIGS. 2-3, the only "security data" that is being exchanged between the client 110 and the tunnel 140 is authentication requests and tokens. Obviously, such exchange of requests, authenticated requests and tokens is performed for purposes of authenticating the client 110 by the tunnel 140 and granting access to private resources/data (this is clearly explained in the above Birrell citation used by the Examiner). Birrell simply does not disclose any utilizing by the tunnel 140 of acquired security data associated with the media peripheral **<u>and</u>** previously acquired security data (associated with a location of previous operation of the media peripheral) to facilitate secure communication.

Therefore, the Applicant maintains that Birrell does not disclose or suggest at least the limitation of "if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network," as recited by the Applicant in independent claim 1.

Accordingly, independent claim 1 is not anticipated by Birrell and is allowable. Independent claims 11 and 18 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11 and 18 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.

B. Rejection of Dependent Claims 2-3, 6, 10, 12-13, 19-20, 23, and 27-28

Based on at least the foregoing, the Applicant believes the rejection of independent claim 1, 11, and 18 under 35 U.S.C. § 102(e) as being anticipated by Birrell has been overcome and request that the rejection be withdrawn. Additionally, claims 2-3, 6, 10, 12-13, 19-20, 23, and 27-28 depend from independent claim 1, 11, and 18, and are, consequently, also respectfully submitted to be allowable.

Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 1-3, 6, 10-13, 18-20, 23, and 27-28.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

In order for a *prima facie* case of obviousness to be established, the Manual of Patent Examining Procedure, Rev. 6, Sep. 2007 ("MPEP") states the following:

> The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

See the MPEP at § 2142, citing *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), and *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval). Further, MPEP § 2143.01 states that "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art" (citing *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007)). Additionally, if a *prima facie* case of obviousness is not established, the Applicant is under no obligation to submit evidence of nonobviousness:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

See MPEP at § 2142.

III. Birell Does Not Render Claims 1-4, 6-7,10-13, 18-21, 23-24, and 27-28 Unpatentable

The Applicant now turns to the rejection of claims 1-4, 6-7,10-13, 18-21, 23-24, and 27-28 as being unpatentable over Birrell. *The Examiner has relied on his arguments stated in pages 5-7 of the Office Action.*

A. Independent Claims 1, 11 and 18

With regard to the rejection of independent claim 1 under 35 U.S.C. § 103(a), the Applicant submits that Birrell does not disclose or suggest at least the limitation of "searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 1.

The Office Action states the following:

> In col. 4 lines 18-27 Birrell discloses:
>
> "(13) At this point, if the client 110 is already known to the proxy server, then proceed with message 209, i.e., request 370 below. Otherwise, in the case where the client is unknown, the redirected browser makes a secure request 330 in a message 203 to the proxy server 143 for the desired resource. In the case, where the client 110 is unknown, the proxy server 143 replies a message 204 to demand that the user makes an authentication request 205 using the checker 141, e.g., a redirect 340 to the checker 141."
>
> This reads on: "searching by the node, for a previously acquired security data" associated with a location of previous operation of the media peripheral.

See the Office Action at pages 5-6. In page 5 of the Office Action, the Examiner equates Applicant's "node" and "media peripheral" to Birrell's tunnel 140 and client 110. In reference to the above Birrell citation used by the Examiner (col. 4, lines 18-27), the

Applicant points out that the tunnel 140 (or any of its modules – checker 141, redirector 142, or proxy 143) does not perform any searching whatsoever. In addition, the only "security data" being exchanged between the client 110 and the tunnel 140 are secure tokens, which are being used for purposes of authenticating the connection. *See* Birrell at FIGS. 2-3. Birrell simply does not disclose that the tunnel 140 performs any searching for a previously acquired security data, which is associated with a location of previous operation of the client 110.

The Office Action also states the following at page 8:

> Note that a message 209 sent from the peripheral to the node disclosed in col. 4 line 47-49 could also be interpreted as an acquired secure data associated with the media peripheral and validating the token 299 disclosed in col. 4 lines 49-51. **The process of token validation would have inherently involve searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral,** and Birrell's disclosure in col. 4 lines 50-64 evidences utilizing by the node, the acquired security data associated with the media peripheral and the previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network.

The Applicant respectfully disagrees. As explained above, message 209 is simply an authentication token, which is sent from the client 110 to the proxy 143 (step 370 in FIG. 3). As known in the art, authentication tokens in token-based systems are used for purposes of authenticating a connection and subsequent information exchange. There is absolutely no support in Birrell (or in any other prior art) that such token would in any way be associated with a location of previous operation of the peripheral, nor is there any reason for such association. *The assertion of inherency (bolded statement above) is specifically traversed herein below.*

Therefore, Birrell does not disclose or suggest at least the limitation of “searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral,” as recited by the Applicant in independent claim 1.

Furthermore with regard to the rejection of independent claim 1 under 35 U.S.C. § 102(e), the Applicant submits that Birrell does not disclose or suggest at least the limitation of “if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network,” as recited by the Applicant in independent claim 1.

The Office Action states the following:

> Similarly, col. 4 lines 18-27 with
>
> "As a result of the interchanges with the checker 141, the client computer can be provided, in step 360, a validation token 299 in message 208. The token can be in the form of an X.500 certificate. Alternatively, the token 299 can be a short-term password to authenticate the user on the HTTPS connection. The short-term password might automatically get installed in the client 110 as a Web "cookie" as a side-effect of the interchange. The message 208 also redirects the browser 111 to further communicate with the proxy server 143.
>
> Therefore, in a next message 209, the client send the request for the resource plus the token 299 to the proxy server 143. When the proxy server 143 receives the message, it validates the token 299. If the token is valid, then the proxy server 143 behaves as a conventional proxy server.
>
> The proxy server 143 forwards the authenticated request 210 to the specified resource 160 inside the firewall 130 using the non-secure HTTP protocol. The resource 160 replies to the request with, for example private data, in message 211. The proxy server 143 then forwards the data, using secure HTTPS protocol, in a message 212 (step 380).

> Subsequent requests for private resources during the session can be handled as follows. The resource is specified in a public message 201 to the redirector 142. The redirector replies message 202. The client 110 now in possession of the token 299 replies message 208 (step 370) causing the further interchange of message 210-212 between the proxy and the server controlling the private resource 160. "
>
> as taught in col. 4 lines 37-64, reads on: "if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network".

See the Office Action at pages 6-7. As already explained above in reference to Birrell's FIGS. 2-3, the only "security data" that is being exchanged between the client 110 and the tunnel 140 is authentication requests and tokens. Obviously, such exchange of requests, authenticated requests and tokens is performed for purposes of authenticating the client 110 by the tunnel 140 and granting access to private resources/data (this is clearly explained in the above Birrell citation used by the Examiner). Birrell simply does not disclose any utilizing by the tunnel 140 of acquired security data associated with the media peripheral **and** previously acquired security data (associated with a location of previous operation of the media peripheral) to facilitate secure communication.

Therefore, the Applicant maintains that Birrell does not disclose or suggest at least the limitation of "if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network," as recited by the Applicant in independent claim 1.

Accordingly, independent claim 1 is not anticipated by Birrell and is allowable. Independent claims 11 and 18 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11 and 18 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.

Therefore, the Applicant submits that claim 1 is allowable. Independent claims 11 and 18 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11 and 18 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1. The Applicant respectfully reserves the right to argue any additional reasons, beyond those set forth above, that support the allowability of claims 1, 11, and 18 should that need arise in the future.

B. Rejection of Dependent Claims 2-4, 6-7, 10, 12-13, 19-21, 23-24, and 27-28

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1, 11 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Birrell has been overcome and requests that the rejection be withdrawn. Additionally, claims 2-4, 6-7, 10, 12-13, 19-21, 23-24, and 27-28 depend from independent claims 1, 11, and 18 and are, consequently, also respectfully submitted to be allowable.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 2-4, 6-7, 10, 12-13, 19-21, 23-24, and 27-28.

IV. Handelman Does Not Render Claims 1, 3, 6-7, 11-13, 18, 20, and 23-24 Unpatentable

The Applicant now turns to the rejection of claims 1, 3, 6-7, 11-13, 18, 20, and 23-24 as being unpatentable over Handelman.

A. Independent Claims 1, 11 and 18

With regard to the rejection of independent claim 1 under 35 U.S.C. § 103(a), the Applicant submits that Handelman does not disclose or suggest at least the limitation of "searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 1.

The Office Action states the following:

> Handelman discloses at least one processor (an system processing a client request, e.g. a system comprising headend that includes Hardware Configuration Provider Unit 70, Fig. 1 or 2) that **acquires security data (a representation of financial transaction details and/or a payment identification code that may be processed to enable billing of the user, [0095]) associated with the media peripheral (STB 45);** said at least one processor searches for a previously acquired security data associated with a location of previous operation of the media peripheral (the headend then processes the payment identification code to bill the user [0095] clearly discloses that the headend must have some previously acquired security data corresponding to the security data. As per location, the examiner points out that in addition to some kind of address present in the previously acquired security data, which must be present for the user to receive billing data, which reads "a previously acquired security data being "associated" with a location of previous operation of the media peripheral, some kind of location of the equipment must be present in the system in order for the Hardware Configuration Provider Unit to be able to receive data).

See the Office Action at pages 9-10 (emphasis added). The Applicant respectfully disagrees with the above argument, especially with the above bolded portion. Referring to FIGS. 1-2 of Handelman, Handelman discloses that the user indicates an agreement to pay for the circuit reconfiguration of the configurable device 60 within the STB 45. **The indication by the user includes information that enables billing of the user, such as financial transaction details and/or payment identification code (which are collectively equated by the Office Action to Applicant's "security information"). Obviously, such information that enables billing of the user (which is equated by the Office Action to Applicant's "security information") is not associated with any location of a previous operation of the STB 45 (equated by the Office Action to Applicant's "media peripheral"). In fact, Handelman's information that enables billing of the user is related to the user, rather than to the STB 45. <u>In response to the argument stated in page 2 of the Office Action,</u> the Applicant points out that even if Handelman's information that enables billing of the user includes the billing address of the user, such address is not necessarily the location of operation of the STB 45. Furthermore, the billing address of the user would not indicate, and would not be associated with, a location of a previous operation of the STB 45.**

The Applicant maintains that Handelman does not disclose or suggest at least the limitation of "searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral," as recited by the Applicant in independent claim 1.

Therefore, the Applicant submits that claim 1 is allowable. Independent claims 11 and 18 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11 and 18 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1. The Applicant respectfully submits that claims 1, 11, and 18 are allowable. The Applicant respectfully reserves the right to argue any additional reasons, beyond those set forth above, that support the allowability of claims 1, 11, and 18 should that need arise in the future.

B. Rejection of Dependent Claims 3, 6-7, 12-13, 20, and 23-24

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1, 11, and 18 under 35 U.S.C. § 103(a) as being unpatentable over Handelman has been overcome and requests that the rejection be withdrawn. Additionally, claims 3, 6-7, 12-13, 20, and 23-24 depend from independent claims 1, 11, and 18 and are, consequently, also respectfully submitted to be allowable.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 3, 6-7, 12-13, 20, and 23-24.

V. Rejection of Dependent Claims 5 and 22

Claims 5 and 22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Handelman in view of Stallings.

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Handelman has been overcome and requests that the rejection be withdrawn. Stallings does not overcome the deficiencies of Handelman. Additionally, claims 5 and 22 depend from independent claims 1 and 18 and are, consequently, also respectfully submitted to be allowable.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 5 and 22.

VI. INHERENCY

The Office Action states the following:

> Thus, operating the peripheral in peripheral's home domain preceding operating the peripheral in a foreign domain (equating the security data comprising MN_NAI value to "a location of the previous operation of the media peripheral"), if not inherent, would have been at least implicit. (page 4)
>
> Paila's disclosure of "attendant merely allows the mobile node's traffic to pass the attendant from this moment on" in paragraph [0053]) inherently includes registering the media peripheral for subsequent operation in the communication network. (page 4)
>
> The process of token validation would have inherently involve searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral, and Birell's disclosure in col. 4 lines 50-64 evidences utilizing by the node, the acquired security data associated with the media peripheral and the previously acquired security data to facilitate secure communication

> between the media peripheral in the home and the communication network 18. (page 8)
>
> (a successful transaction, which *inherently* would involve at least associating and comparing the acquired security data and the previously acquired security data, results in data being communicated to the media peripheral, e.g. [0099]) (page 10)

See the Office Action at pages 4, 8, and 10. Initially, regardless of whether the above statements are true or not, the Applicant notes that it appears that additional claims (such as at least independent claims 1, 11 and 18) are being rejected over Paila (pages 3-4 of the Office Action), over Birrell (page 8 of the Office Action), and over Handelman (page 10 of the Office Action) based on inherency.

The Applicant submits that a rejection based on inherency must include a statement of the rationale or evidence tending to show inherency. *See* Manual of Patent Examining Procedure at § 2112. "The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic." *See id. citing In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993).

> To establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. **Inherency, however, may not be established by probabilities or possibilities.** The mere fact that a certain thing may result from a given set of circumstances is not sufficient.

In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999). The Applicant respectfully submits that neither the cited references (such as Paila, Birrell, and Handelman) nor the Office Action "make[s] clear that the missing descriptive matter," said to be inherent "is necessarily present in" the references cited in the Office Action.

A rejection based on inherency must be based on factual or technical reasoning:

> In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teaching of the applied prior art.

Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990).

The Applicant respectfully submits that the Office Action does not contain a basis in fact and/or technical reasoning to support the rejection based on inherency. Instead, as recited above, at least claims 1, 11 and 18 of the present application stand rejected based on a conclusory statements of inherency or implicitness, rather than upon a "basis in fact and/or technical reasoning." Accordingly, the Applicant respectfully submits that, absent a "basis in fact and/or technical reasoning" for the rejection of record, that rejection should be reconsidered and withdrawn.

VII. Allowable Subject Matter

Claims 8 and 25 have been objected to. The Applicant has cancelled the objected to claims 8 and 25, and has added new independent claims 29 and 36 corresponding to claims 8 and 25. New dependent claims 30-35 and 37-43 correspond to dependent claims 2-5, 9-10, 19-22, and 26-28.

CONCLUSION

Based on at least the foregoing, the Applicant believes that all pending claims 1-7, 9-24, and 26-43 are in condition for allowance. If the Examiner disagrees, the Applicant respectfully requests a telephone interview, and request that the Examiner telephone the undersigned Attorney at (312) 775-8176.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

A Notice of Allowability is courteously solicited.

Respectfully submitted,

Date: 30-OCT-2008

/Ognyan I. Beremski/
Ognyan Beremski, Esq.
Registration No. 51,458
Attorney for Applicant

McAndrews, Held & Malloy, Ltd.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
(312) 775-8000